WHAT WE CLAIM IS:

1. A detection system for detecting intrusive behavior in a first session on a computer, said first session comprising a plurality of applications invoked on said computer, and said computer having a computer operating system, said detection system comprising:

(a) a plurality of first application profiles, wherein each of said first application profile comprises a plurality of first data strings, wherein each first data string comprises a sequential mapping of instructions passed from one of said plurality of applications to the computer operating system during a second session on the computer;

(b) a plurality of second application profiles, wherein each second application profile comprises a plurality of application segments, wherein each application segment comprises a pre-determined number of second data strings, wherein each second data string comprises a sequential mapping of instructions passed from one of said applications to the computer operating system during the first session on the computer;

(c) an application counter;

(d) a plurality of segment counters, wherein each segment counter corresponds to one of the second application profiles;

(e) a plurality of data string counters, wherein each data string counter corresponds to one of the application segments in the plurality of application segments;

(f) an equality matcher, wherein for each application segment, each second data string is compared to the plurality of first data strings comprising a corresponding application profile, and wherein if the second data string is not equal to any of the first data strings the equality matcher increments an associated data string counter; and

(g) a temporal locality identifier, wherein the temporal locality identified labels the first session intrusive if a ratio of the segment counter to a total number of segments in an associated second application profile exceeds an application threshold and wherein the first session is labeled intrusive if a ratio of the application counter to a total number of applications exceeds a session threshold, wherein the application counter is incremented if a ratio of an associated segment counter to a total number of segments in an associated second application profile exceeds a segment threshold, wherein the associated segment counter is incremented if a ratio of an associated data string counter to the pre-determined number of data strings comprising the segment exceeds an associated data string threshold.

2. The detection system of claim 1, wherein the second session comprises non-intrusive behavior.

3. The detection system of claim 1, wherein the computer operating system comprises a UNIX operating system and the sequential mapping of instructions comprise a sequential mapping of UNIX system calls.

4. The detection system of claim 1, wherein the computer operating system comprises a Windows NT operating system, and wherein the sequential mapping of instructions comprises a sequential mapping of object requests.

5. The detection system of claim 1, wherein the first plurality of application profiles and second plurality of application profiles are created by a data pre-processor application.

6. The detection system of claim 5, wherein the data pre-processor receives input from an auditing system integral to the computer operating system.

7. The detection system of claim 5, wherein the data pre-processor creates the second plurality of application profiles in real-time.

8. The detection system of claim 5, wherein the equality matcher and the temporal locality identifier receive input from the plurality of second application profiles in real-time.

9. The detection system of claim 1, characterized by a false positive rate less than 4.0% and a false negative rate less than 11%.

10. The detection system of claim 1, characterized by a false positive rate less than 3.0% and a false negative rate less than 13%.

11. The detection system of claim 1, characterized by a false positive rate less than 2.5% and a false negative rate less than 30%.

12. A method for detecting intrusive behavior in a first session on a computer, said first session comprising a plurality of applications invoked on said computer, and said computer having a computer operating system, said method comprising the steps of:

(a) creating a plurality of first application profiles, wherein each said first application profile comprises a plurality of first data strings, wherein each first data string comprises a sequential mapping of instructions passed from one of said plurality of applications to the computer operating system during a second session on the computer;

(b) creating a plurality of second application profiles, wherein each second application profile comprises a plurality of application segments, wherein each application segment comprises a pre-determined number of second data strings, wherein each second data string comprises a sequential mapping of instructions passed from one of said applications to the computer operating system during the first session on the computer;

(c) initializing an application counter;

(d) initializing a plurality of segment counters, wherein each segment counter corresponds to one of the second application profiles;

(e) initializing a plurality of data string counters, wherein each data string counter corresponds to one of the application segments in the plurality of application segments;

(f) performing an equality matching algorithm, wherein for each application segment, each second data string is compared to the plurality of first data strings comprising a corresponding application profile, and wherein if the second data string is not equal to any of the first data strings an associated data string counter is incremented; and

(g) performing a temporal locality identifying algorithm, wherein the first session is labeled intrusive if a ratio of the segment counter to a total number of segments in an associated second application profile exceeds an application threshold and wherein the first session is labeled intrusive if a ratio of the application counter to a total number of applications exceeds a session threshold, wherein the application counter is incremented if a ratio of an associated segment counter to a total number of segments in an associated second application profile exceeds a segment threshold, wherein the associated segment counter is incremented if a ratio of an associated data string counter to the pre-determined number of data strings comprising the segment exceeds an associated data string threshold.

13. The method of claim 12, wherein the second session comprises non-intrusive behavior.

14. The method of claim 12, wherein the computer operating system comprises a UNIX operating system and the sequential mapping of instructions comprise a sequential mapping of UNIX system calls.

15. The method of claim 12, wherein the computer operating system comprises a Windows NT operating system, and wherein the sequential mapping of instructions comprises a sequential mapping of object requests.

16. The method of claim 12, wherein the first plurality of application profiles and second plurality of application profiles are created by a data pre-processor application.

17. The method of claim 16, wherein the data pre-processor receives input from an auditing system integral to the computer operating system.

18. The method of claim 16, wherein the data pre-processor creates the second plurality of application profiles in real-time.

19. The method of claim 16, wherein the equality matching algorithm and the temporal locality identifying algorithm receive input from the second plurality of application profiles in real-time.

20. The method of claim 12, characterized by a false positive rate less than 4.0% and a false negative rate less than 11%.

21. The method of claim 12, characterized by a false positive rate less than 3.0% and a false negative rate less than 13%.

22. The detection system of claim 12, characterized by a false positive rate less than 2.5% and a false negative rate less than 30%.

23. A detection system for detecting intrusive behavior in a session on a computer, said session comprising a plurality of applications invoked on said computer, and said computer having a computer operating system, said detection system comprising:

(a) a plurality of neural networks, wherein each neural network is trained to identify a pre-determined behavior pattern for a corresponding one of the plurality of applications;

(b) a plurality of application profiles, wherein each application profile comprises a plurality of application data for a corresponding one of the plurality of applications, wherein said application data is collected during the session;

(c) a temporal locality identifier, wherein when one of the plurality of application profiles is sequentially input to a corresponding one of the plurality of neural networks the neural network outputs a behavior indicator for each of the plurality of data strings in the application profile, and wherein if the behavior indicator meets a pre-determined criteria, a counter is incremented, and wherein if the counter has a high rate of increase the temporal locality identifier labels the application behavior intrusive, and wherein if a predetermined percentage of application behaviors are intrusive the session behavior is labeled intrusive.

24. The detection system of claim 23, wherein the pre-determined behavior pattern comprises a non-intrusive behavior.

25. The detection system of claim 23, wherein the computer operating system comprises a UNIX operating system and the application data comprises a distance between a sequential mapping of UNIX system calls made by a corresponding one of the plurality of applications and a pre-defined string of UNIX system calls.

26. The detection system of claim 23, wherein the computer operating system comprises a Windows NT operating system, and the application data comprises a distance between a sequential mapping of object requests made by a corresponding one of the plurality of applications and a pre-defined string of object requests.

27. The detection system of claim 23, wherein the plurality of application profiles is created by a data pre-processor application.

28. The detection system of claim 27, wherein the data pre-processor receives input from an auditing system integral to the computer operating system.

29. The detection system of claim 27, wherein the data pre-processor creates the plurality of second application profiles in real-time.

30. The detection system of claim 27, wherein the plurality of trained neural networks receive input from the plurality of application profiles in real-time.

31. The detection system of claim 23, wherein the pre-determined behavior pattern comprises a non-intrusive behavior and said system is characterized by a false positive rate less than 2.5% and a false negative rate less than 30%.

32. The detection system of claim 23, the pre-determined behavior pattern comprises a intrusive behavior and said system is characterized by a false positive rate less than 10.0% and a false negative rate less than 9.0%.

33. The detection system of claim 23, wherein the plurality neural network comprises a plurality of backpropogation neural networks.

34. The detection system of claim 33, wherein each neural network in the plurality of backpropogation neural networks comprises an input layer, a hidden layer and an output layer.

35. The detection system of claim 34, wherein a number of nodes in the hidden layer is determined by testing a plurality of cases for each neural network in the plurality of backpropogation neural networks and selecting the case wherein the corresponding neural network has a highest accuracy rate.

36. The detection system of claim 23, wherein the plurality of neural networks comprises a plurality of recurrent neural networks.

37. A method for detecting intrusive behavior in a session on a computer, said session comprising a plurality of applications invoked on said computer, and said computer having a computer operating system, said method comprising the steps of:

(a) training a plurality of neural networks, wherein each neural network is trained to identify a pre-determined behavior pattern for a corresponding one of the plurality of applications;

(b) creating a plurality of application profiles, wherein each application profile comprises a plurality of application data for a corresponding one of the plurality of applications, wherein said application data is collected during the session;

(c) performing a temporal locality identifying algorithm, wherein when one of the plurality of application profiles is sequentially input to a corresponding one of the plurality of neural networks the neural network outputs a behavior indicator for each of the plurality of data strings in the application profile, and wherein if the behavior indicator meets a pre-determined criteria, a counter is incremented, and wherein if the counter has a high rate of increase the temporal locality identifier labels the application behavior intrusive, and wherein if a predetermined percentage of application behaviors are intrusive the session behavior is labeled intrusive.

38. The method of claim 37, wherein the pre-determined behavior pattern comprises a non-intrusive behavior.

39. The method of claim 37, wherein the computer operating system comprises a UNIX operating system and the application data comprises a distance between a sequential mapping of UNIX system calls made by a corresponding one of the plurality of applications and a pre-defined string of UNIX system calls.

40. The method of claim 37, wherein the computer operating system comprises a Windows NT operating system, and the application data comprises a distance between a sequential

mapping of object requests made by a corresponding one of the plurality of applications and a pre-defined string of object requests.

41. The method of claim 37, wherein the plurality of application profiles is created by a data pre-processor application.

42. The method of claim 41, wherein the data pre-processor receives input from an auditing system integral to the computer operating system.

43. The method of claim 41, wherein the data pre-processor creates the plurality of second application profiles in real-time.

44. The method of claim 41, wherein the plurality of trained neural networks receive input from the plurality of application profiles in real-time.

45. The method of claim 37, wherein the pre-determined behavior pattern comprises a non-intrusive behavior and said system is characterized by a false positive rate less than 2.5% and a false negative rate less than 30%.

46. The method of claim 37, the pre-determined behavior pattern comprises a intrusive behavior and said system is characterized by a false positive rate less than 10.0% and a false negative rate less than 9.0%.

47. The method of claim 37, wherein the plurality neural network comprises a plurality of backpropogation neural networks.

48. The method of claim 37, wherein each neural network in the plurality of backpropogation neural networks comprises an input layer, a hidden layer and an output layer.

49. The method of claim 48, wherein a number of nodes in the hidden layer is determined by testing a plurality of cases for each neural network in the plurality of backpropogation neural

networks and selecting the case wherein the corresponding neural network has a highest accuracy rate.

50. The method of claim 37, wherein the plurality of neural networks comprises a plurality of recurrent neural networks.